# SwA Summer 2012 Working Group Sessions At-A-Glance Agenda (as of June 20, 2012)

MITRE-1, 7525 Colshire Drive, McLean, VA 22102

| 26 June (Tuesday)<br>8:30 AM – Registration | | 27 June (Wednesday)<br>8:30 AM – Registration | 28 June (Thursday)<br>8:30 AM – Registration |
|---|---|---|---|
| 9:00 AM Opening | | 9:00 AM Opening | 9:00 AM Opening |
| Overview – Joe Jarzombek, DHS NCSD<br>Education and Educational Initiatives Part 1 – Nancy Mead, Dan Shoemaker and Art Conklin<br>Synergy with the NICE initiative – Margaret Maxson | | Emerging Requirements for Software Assurance – Don Davidson & Jon Boyens | Technology Demonstrations Overview – Joe Jarzombek<br>New Technology for Zero-Day Attack Protection - Fire Tower |
| 10:00 - 10:30 AM Break | | 10:00 - 10:30 AM Break | 9:45 – 10:15 AM Break |
| Education and Educational Initiatives Part 1– Nancy Mead, Dan Shoemaker and Art Conklin | | Software Assurance Technologies/Validating Requirements: Technology Enabled Testing Landscape(Software Assurance) - Joe Jarzombek | Technology Demonstrations<br>Pattern analysis and software remediation in the context of legacy modernization - The Software Revolution Inc.<br>Tool Output Integration Framework (TOIF) – KDM Analytics<br>Software Assurance Visualization (SwA-Vis) - Applied Visions |
| NOON – 1:30 Lunch | | NOON – 1:30 Lunch | 12:30 Wrap Up |
| Leveraging SwA Automation throughout the SDLC- Don Davidson and Michele Moss (Auditorium) | UK Approach to Trustworthy Software Training, Education and Awareness – Ian Bryant (1H300) | Contract Language - Joe Jarzombek<br>Software Assurance Research and Development Needs<br>Software IDs | |
| 3:00 – 3:30 PM Break | | 3:00 – 3:30 PM Break | |
| SwA Automation Use Cases & Practices – Bob Martin & Richard Struse (Auditorium) | Education and Educational Initiatives Part 2 – Nancy Mead, Dan Shoemaker and Art Conklin (1H300) | Cyber Assessment Risk Management Approach (CARMA) - TBD<br>Measuring the Outcomes of SwA Practices - James Lindley | |
| 5:00 PM Wrap-Up | | 5:00 PM Wrap-Up | |

# SwA Summer 2012 Working Group Sessions At-A-Glance Agenda (as of June 20, 2012)

MITRE-1, 7525 Colshire Drive, McLean, VA 22102

**Workforce, Education, and Training Working Group (WET) Discussion Topics:**

- **Synergy with the National Initiative for Cybersecurity Education(NICE).** We will understand the current status and plans of NICE and discuss the impact it can have on educational needs for SwA. How does one "get involved" with any NICE revision efforts? How can we add roles and functions that are definitely needed but not currently included?
- **UK Approach to Trustworthy Software Training, Education and Awareness.** Software forms an intrinsic and indivisible element of the emergent cyberspace domain, yet is contingent upon a variety of diverse participants – private firms, non-profit organizations, governments and individuals. It is therefore vital that intrinsic challenges to software are recognized and treated such that a trustworthy software ecosystem can be formed. This presentation discusses the current UK activities towards providing a consensus, standards driven approach to improvement of training, education and awareness in trustworthy software. Ian Bryant of the UK Software Security, Dependability and Resilience Initiative (SSDRI) will present a summary of the segmentation model proposed to UK Training, Education and Awareness in Trustworthy Software, to allow discussion of synergies and potential opportunities for burden sharing.
- **Hiring software assurance professionals.** We will discuss and identify the requisite skills, keywords and text to use in job descriptions, keywords to look for in resumes, and example interview questions.
- Recommended reading – There has been much discussion of a Top 10 list of some sort. We will review that discussion and develop a candidate list.
- **CS2013 Review.** CS2013 is the undergraduate computer science curriculum revision, which is of great importance for software assurance going forward. It will be in review until July, so the working group will use this session to collect feedback for submission. See the attached word document for *Software Assurance Additions to the Core Knowledge Areas*. The draft undergraduate computer science curriculum revision by the ACM/IEEE-CS Joint Task Force has great importance for software assurance, so the working group will discuss our recommendations. To get prepared for that discussion, please review the CS2013 Strawman at http://ai.stanford.edu/users/sahami/CS2013/.

**Leveraging SwA Automation throughout the SDLC Session Overview**: This session will introduce the DoD efforts to address Software Assurance during system development milestone decisions using a Program Protection Plan (PPP), discuss initial industry feedback on DoD's PPP template, and create a proof of concept approach for leveraging leading industry frameworks and guidance to create additional resources to ease the discussions between acquirers and suppliers during development and acquisition milestones.

**Software Assurance Automation**: We are planning discussions of several use cases for SwA Automation. We will also consider the SwA conditions and evidence for placing an app in an app store, and SwA rating systems for determining which weaknesses are most important. Next, we will cover the newly updated "Key Practices" Pocket Guide draft. We will wrap up with a discussion of including security automation standards in a cyber campaign and kill chain, as well as commercial offerings and operations and development.

**Government and Industry SwA/Software Supply Chain Standards Update**: The U.S. government and national and multinational industry partners are have on-going efforts to identify and understand risks associated with a global information and communications technology (ICT) supply chain and to implement and mature practices to manage the risk.  This session at the June Working Group Sessions will provide updates on the progress made to document required and expected practices.

**Contract Language to Implement Software Assurance:** We will discuss potential contract language to address the following concerns: What has the supplier checked for? What can be asked for? We will use as a reference the study by Aspect Security and Sonatype: The Unfortunate Reality of Insecure Libraries

**Software Assurance Research and Development Needs:** The goal of this session is to develop a prioritized list of Software Assurance needs. These needs must be clearly identified and prioritized in order to discover relevant R&D technologies that might satisfy them. The Research and Standards Integration (RSI) program has an R&D mission to transition leading edge technologies into operational environments. DART3 (DHS Assistant for Research and development Tracking and Technology Transition) is a web-based semantic tool and repository designed to capture US Federally-funded R&D project descriptions and R&D requirements to facilitate technology transitions. This talk will present the RSI R&D transition mission, the DART3 tool, and a preliminary list of needs of the Software Assurance community. A group discussion is encouraged to develop a prioritized list of Software Assurance requirements.

**Cyber Assessment Risk Management Approach (CARMA) and SwA:** We will discuss the role of Software Assurance in DHS's CARMA initiative. CARMA is a top-down approach to cyber infrastructure risk assessment and management that DHS's National Cyber Security Division (NCSD) leverages in its engagement with critical infrastructure and key resources (CIKR) sectors. As the cybersecurity discipline has become a key focal point of national and homeland security discussions, CIKR sector entities and governments have increased their demand for understanding cyber risks. In response, the NCSD has leveraged its unique public-private sector partnership role as a mechanism for establishing approaches to highlight national-level cybersecurity risks and concerns in a national-level approach to cyber risk management that can initiate sector, sub-sector, regional, or State and local strategic cyber risk management efforts. CARMA consists of five stages and can integrate into established cyber risk management frameworks or be used as a foundation for a broader risk management framework. The processes and outputs specific to each stage can be used to scope, identify, and address cyber risk at the national-, sector-, or enterprise-level. We will discuss the potential synergies between the SwA process and practices and the CARMA effort.

**New Technology for Zero-Day Attack Protection:** There are numerous ways for malicious software to gain access to your computer, but to assure that they remain there they often use a common trick: creating an auto-run entry on your computer. An auto-run entry allows software of all types, malicious or safe, to establish persistence on a computer by instructing the operating system to automatically execute this software during every system boot up.  This new technology for Zero-Day Attack Protection is non-signature based, light weight, and real-time It is not behavior based; not scanning based; not reputation based.  This malware discovery technology does not use signature-based detection; is independent of service pack updates for the operating system; and does not require prior knowledge of exploits. This facilitated presentation/demonstration/discussion in which attendees are asked to provide input and feedback on capabilities to address Advanced Persistent Threats.

**Pattern analysis and software remediation in the context of legacy modernization:** We will see a demonstration of new work on language neutral tunable pattern analysis techniques for software weakness detection and remediation. TSRI is showing it to elicit comments feedback and to discover if there is interest in collaborative work from other members of the SwA community.

**Tool Output Integration Framework (TOIF) and Software Assurance Visualization (SwA-Vis):** No single software assurance tool is likely to identify all security weaknesses. This session will describe two related DHS Science and Technology Directorate (S&T) initiatives that are aimed at using multiple security analysis tools to increase coverage: TOIF and SwA-Vis. TOIF is an open-source standard-based framework for integrating and normalizing the weakness findings reported by multiple detection tools (commercial and open source) and SwA-Vis is a tool to visualize the security tool findings in a single unified interface, putting them into proper context for effective triage and mitigation. This session will demonstrate the current status of these projects as well as discuss how users can access this technology. We will be eliciting feedback during this session with respect to the presented functionality and the utility to the audience. Input from attendees will be used to guide future development.